

NETWORK PACKET ANALYSIS USING WIRESHARK

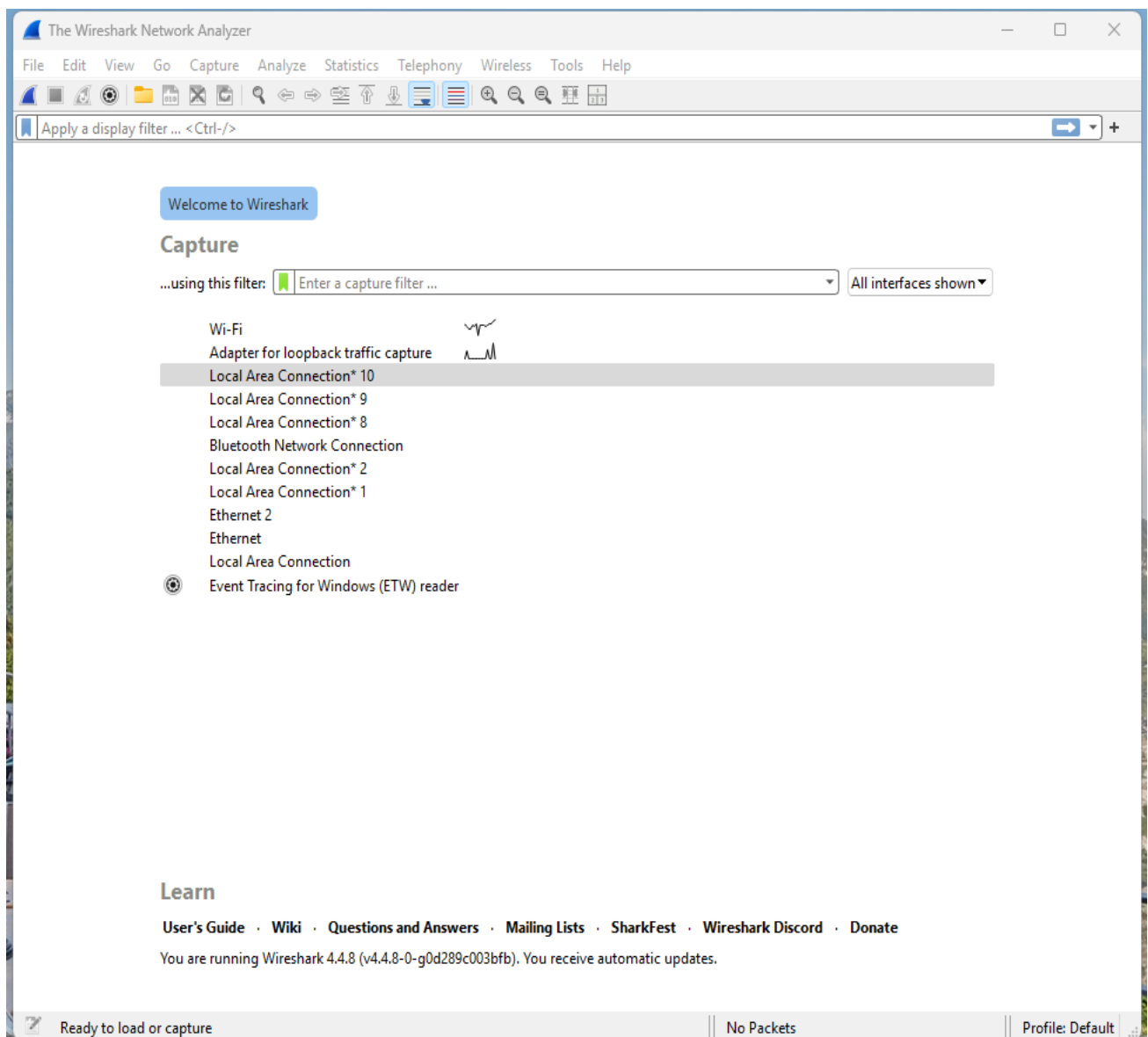
PREPARED BY : LOVEPREET SINGH

BTECH 7TH SEMSTER

TOPIC - NETWORK SECURITY ANALYSIS

SETUP

- **Capture Interface** : WiFi (en0)
- **No of packets Captured** : 15545
- **File Name** : Network_packets.png



FINDINGS

◆ HTTP Filters

1) Filter Used: http

- **Observation:** Captures all HTTP traffic (requests and responses).
- **Security Risk:** HTTP is unencrypted; attackers can sniff usernames, passwords, and data.
- **Recommendation:** Replace HTTP with HTTPS; block plaintext HTTP if possible.

The image displays a Wi-Fi network traffic capture window. The top section shows a list of captured packets, with the first three being HTTP requests. The bottom section shows the details of the first packet, which is an HTTP GET request for /connecttest.txt. The packet details include the Ethernet II header, Internet Protocol Version 6 header, and Hypertext Transfer Protocol header. The packet is captured on interface \Device\NPF_{2630B4FA-BA28-4787-904F-8698B3585}.

No.	Time	Source	Destination	Protocol	Length	Info
156.894363	2481:4900:1c73:76c4...	2680:1417:55:174c...	HTTP	186	GET /connecttest.txt HTTP/1.1	
156.894462	192.168.1.3	96.17.168.107	HTTP	165	GET /connecttest.txt HTTP/1.1	
9574.156.987136	96.17.168.107	192.168.1.3	HTTP	241	HTTP/1.1 200 OK (text/plain)	
9578.156.987990	2680:1417:55:174c...	2481:4900:1c73:76c4...	HTTP	261	HTTP/1.1 200 OK (text/plain)	
18423.175.944591	2481:4900:1c73:76c4...	2680:1861:10:3:11	HTTP	346	GET /captureportal/generate_204 HTTP/1.1 [Illegal Segments]	
18443.176.137814	2680:1861:10:3:11	2481:4900:1c73:76c4...	HTTP	333	HTTP/1.1 204 No Content	

Frame 9578: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface \Device\NPF_{2630B4FA-BA28-4787-904F-8698B3585}

Ethernet II, Src: 14:04:24:19:06:a9, Dst: 38:0d:13:36:25:58

Internet Protocol Version 6, Src: 2481:4900:1c73:76c4:e8bb:f166:556c:5f43, Dst: 2680:1417:55:174c:9c63

Transmission Control Protocol, Src Port: 56798, Dst Port: 80, Seq: 1, Ack: 1, Len: 112

Hypertext Transfer Protocol

0000 38 bd 13 36 25 58 14 46 24 19 06 a9 86 dd 00 01 0-GRP: \$.....
0010 44 c9 00 04 06 40 24 01 49 00 1c 73 7d c4 e8 bb 0-@I:s}...
0020 f1 66 55 6c 5f 43 26 00 14 17 00 55 00 00 00 00 fuL_C@...U....
0030 00 00 17 4c 9c 63 dd de 00 50 64 bb d3 26 db 6f ...Lc...Pd-&o
0040 7c 85 50 18 00 ff 52 88 00 00 47 45 54 20 2f 63 |P...R...GET /c
0050 6f 6e 6e 65 63 74 74 65 73 74 2e 74 70 74 20 40 onnecte st.txt W
0060 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 TTP/L..Connect
0070 69 6f 6e 3a 20 43 6c 6f 73 65 0d 0a 55 73 65 72 ion: Clo se -User
0080 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 -Agent: Microsof
0090 74 20 4e 43 53 49 0d 0a 48 6f 73 74 3a 20 69 70 t.NCSI: Host: ip
00a0 76 36 2e 6d 73 65 74 63 6f 6e 6e 65 63 74 74 65 v6.msfc connecte
00b0 73 74 2e 63 6f 6d 0d 0a 0d 0a st.com ...

2) Filter Used: http.request.method == "GET"

- **Observation:** Shows all GET requests (retrieving resources).
- **Security Risk:** Sensitive information may be leaked in URL query strings (e.g., tokens, session IDs).
- **Recommendation:** Avoid sending sensitive data in GET requests; enforce POST with encryption.

traffic_filters.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method=="GET"

No.	Time	Source	Destination	Protocol	Length	Info
5879	98.808446	2401:4900:1c73:7dc4...	2600:140f:c400::173...	HTTP	562	GET / HTTP/1.1
5937	99.091501	2401:4900:1c73:7dc4...	2600:140f:c400::173...	HTTP	474	GET /favicon.ico HTTP/1.1

> Frame 5879: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface 0
> Ethernet II, Src: 14:d4:24:19:d6:a9, Dst: 30:bd:13:36:25:50
> Internet Protocol Version 6, Src: 2401:4900:1c73:7dc4:7cdb:ae6:e5:1, Dst: 2600:140f:c400::173:1
> Transmission Control Protocol, Src Port: 56146, Dst Port: 80, Seq: 123456789
> Hypertext Transfer Protocol
 > GET / HTTP/1.1\r\n
 Host: www.example.com\r\n
 Connection: keep-alive\r\n
 Upgrade-Insecure-Requests: 1\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8\r\n
 Referer: https://www.bing.com/\r\n
 [Response in frame: 5929]
 [Full request URI: http://www.example.com/]

0000 30 bd 13 36 25 50 14 d4 24 19 d6 a9 86 d0 60 0a 00 6%P.
0010 09 28 01 fc 06 40 24 01 49 00 1c 73 7d c4 7c db ..(...@\$.
0020 0a e6 e5 70 29 95 26 00 14 0f c4 00 00 00 00 00 ...p)&
0030 00 00 17 3c ac 0a db 52 00 50 a6 b9 9b 76 a0 ab ...<...f
0040 b9 bd 50 18 00 ff 25 1f 00 00 47 45 54 20 2f 20 ..P...%
0050 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1..
0060 77 77 77 7e 65 78 61 6d 70 6c 65 2e 63 6f 6d 0d www.exar
0070 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 ..Connect
0080 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 p-alive
0090 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 -Insecu
00a0 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e ts: 1..l
00b0 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil
00c0 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows
00d0 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 70 Win64;
00e0 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 leWebKit
00f0 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 (KHTML,
0100 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 33 39 2e 30 ko) Chro
0110 2e 30 2e 30 20 53 61 66 61 72 69 2f 35 33 37 2e .0.0 Sat
0120 33 36 20 45 64 67 2f 31 33 39 2e 30 2e 30 2e 30 36 Edg/
0130 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 ..Accept
0140 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f tml,app
0150 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 xhtml+xr
0160 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c ation/xr
0170 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 image/av
0180 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 /webp,ir
0190 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 ,/*;q=t
01a0 63 61 74 69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 cation/
01b0 63 68 61 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e change;
01c0 37 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 7..Refer

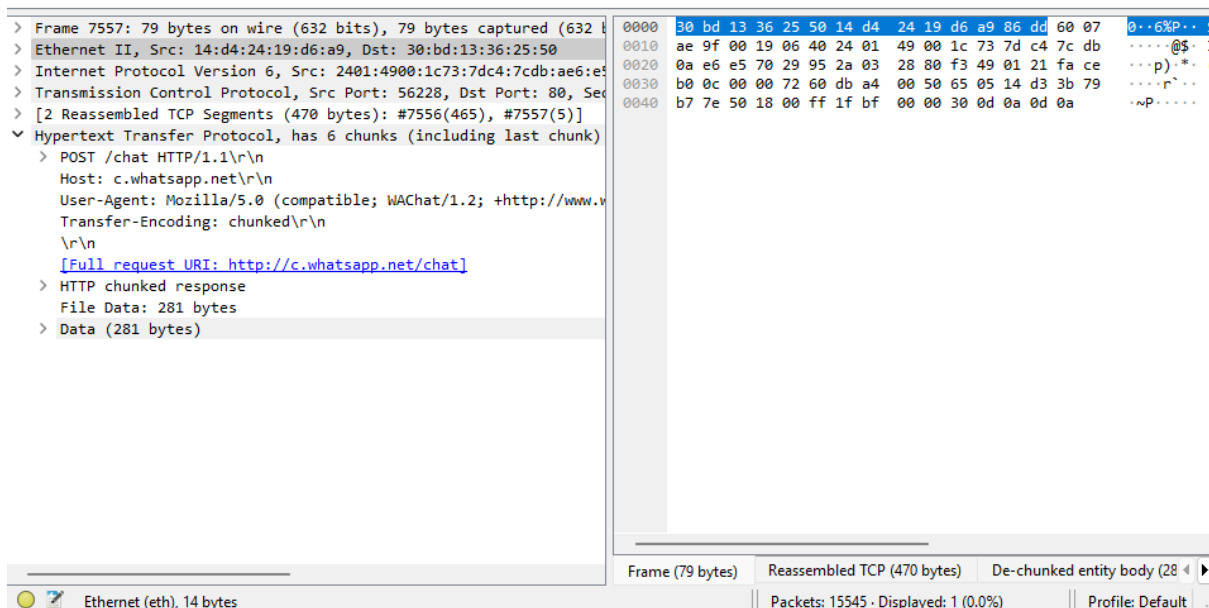
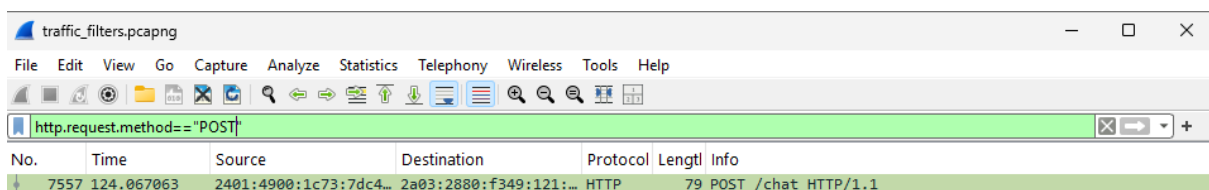
Ethernet (eth), 14 bytes

Packets: 15545 · Displayed: 2 (0.0%)

Profile: Default

3) Filter Used: http.request.method == "POST"

- **Observation:** Captures POST requests (data submissions).
- **Security Risk:** If unencrypted, sensitive form data (credentials, personal data) may be exposed.
- **Recommendation:** Ensure POST requests are always sent via HTTPS.



4) Filter Used: http.response.code >= 400

- **Observation:** Identifies error responses (client and server errors).
- **Security Risk:** Frequent 500-series errors may expose server misconfigurations; 404 scans could indicate reconnaissance attempts.
- **Recommendation:** Monitor error patterns and harden servers against scans.

The image shows a Wireshark packet capture analysis. The top pane displays a list of filtered packets where the filter is `http.response.code >= 400`. Two packets are visible:

No.	http.response.code.desc	Destination	Protocol	Length	Info
5982	100.374646	2600:140f:c400::173...	HTTP	290	HTTP/1.1 404 Not Found (text/html)
8328	134.032706	2600:140f:c400::173...	HTTP	582	HTTP/1.0 408 Request Time-out (text/html)

The bottom pane shows the details of the selected packet (No. 5982). The left pane displays the packet structure:

- > Frame 5982: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits) on interface 0
- > Ethernet II, Src: 30:bd:13:36:25:50, Dst: 14:d4:24:19:d6:a9
- > Internet Protocol Version 6, Src: 2600:140f:c400::173c:ac0a, Dst: 2401:4900:1c73:7dc4::1
- > Transmission Control Protocol, Src Port: 80, Dst Port: 56146, Seq: 2600:140f:c400::173c:ac0a, Win: 0, Len: 290
- > [2 Reassembled TCP Segments (1648 bytes): #5981(1432), #5982(216)]
- > Hypertext Transfer Protocol
 - > HTTP/1.1 404 Not Found\r\n
 - Accept-Ranges: bytes\r\n
 - Content-Type: text/html\r\n
 - ETag: "84238dfc8092e5d9c0dac8ef93371a07:1736799080.121134"\r\n
 - Last-Modified: Mon, 13 Jan 2025 20:11:20 GMT\r\n
 - Server: AkamaiNetStorage\r\n
 - Content-Length: 1256\r\n
 - Expires: Tue, 26 Aug 2025 07:59:57 GMT\r\n
 - Cache-Control: max-age=0, no-cache, no-store\r\n
 - Pragma: no-cache\r\n
 - Date: Tue, 26 Aug 2025 07:59:57 GMT\r\n
 - Connection: keep-alive\r\n
 - \r\n
 - [Request in frame: 5937]
 - [Time since request: 1.283145000 seconds]
 - [Request URI: /favicon.ico]
 - [Full request URI: http://www.example.com/favicon.ico]
 - File Data: 1256 bytes
- > Line-based text data: text/html (46 lines)

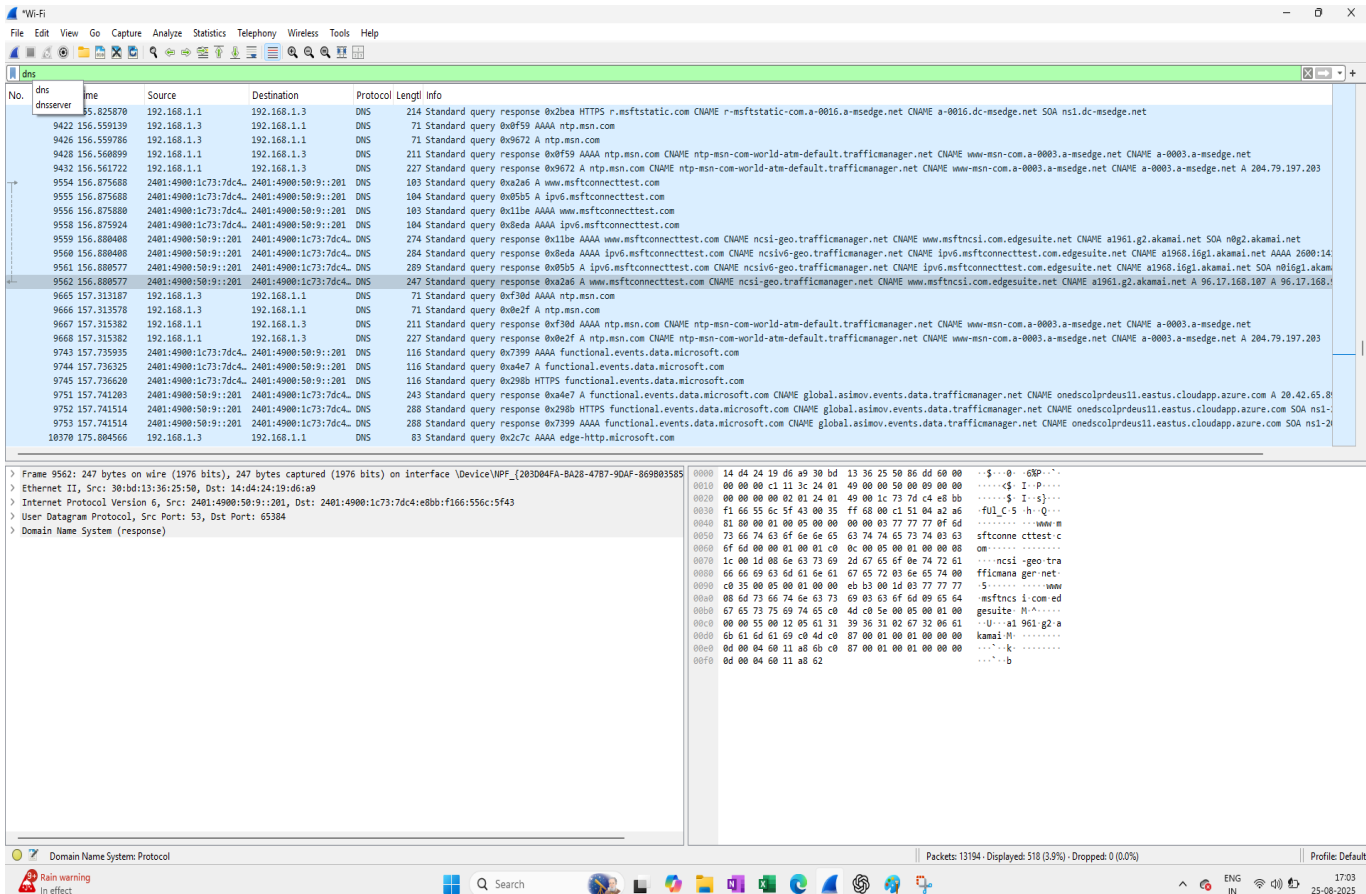
The right pane shows the raw packet data in hexadecimal and ASCII. The ASCII column shows the beginning of the HTML response body, which is mostly garbled due to the 404 status.

At the bottom, the status bar indicates: Status Code: Unsigned integer (24 bits), Packets: 15545 - Discolored: 2 (0.0%), Profile: Default.

DNS Filters

1) Filter Used: dns

- **Observation:** Captures all DNS queries and responses.
- **Security Risk:** Attackers can perform DNS tunneling or track domains being queried.
- **Recommendation:** Enable DNSSEC or encrypted DNS (DoH/DoT).



The image displays a Wi-Fi network traffic capture window, likely from a tool like Wireshark. The main pane shows a list of captured packets, with the DNS filter applied. The list includes various DNS queries and responses, such as standard queries for ntp.msn.com, ipv6.msftconnecttest.com, and functional.events.data.microsoft.com. The packet details pane on the right shows the structure of a DNS response, including the header, question, answer, and authority sections. The packet list pane on the left shows the packet number, time, source, destination, protocol, and length. The packet details pane on the right shows the packet structure, including the header, question, answer, and authority sections. The packet list pane on the left shows the packet number, time, source, destination, protocol, and length. The packet details pane on the right shows the packet structure, including the header, question, answer, and authority sections.

Frame 9562: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits) on interface 'Device\NPF_{203004FA-BA28-4787-9DAF-869803585} (0.0.0.0) [Ethernet II, Src: Rain Warning (08:00:00:00:00:00), Dst: Rain Warning (08:00:00:00:00:00)]

Ethernet II, Src: Rain Warning (08:00:00:00:00:00), Dst: Rain Warning (08:00:00:00:00:00)

Internet Protocol Version 6, Src: 2401:4900:50:9::201, Dst: 2401:4900:1c73:7dc4::e8bb:f166:55c:5f43

User Datagram Protocol, Src Port: 53, Dst Port: 65384

Domain Name System (response)

0000 14 04 24 19 d6 a9 30 bd 13 36 25 50 06 dd 00 00 ...\$...0...6SP...
0010 00 00 00 c1 11 3c 24 01 49 00 00 50 00 09 00 00\$ I-P...
0020 00 00 00 00 02 01 24 01 49 00 1c 73 7d c4 e8 b0\$ I-s}...
0030 f1 66 55 6c 5f 43 00 35 ff 68 00 c1 51 04 a2 a6 ...ful_C 5 -h-Q...
0040 81 00 00 01 00 05 00 00 00 00 03 77 77 0f 6dwww-m
0050 73 66 74 63 6f 6e 65 63 74 74 65 73 74 03 63 ...sftconne cttest c
0060 6f 6d 00 00 01 00 01 c0 0c 00 05 00 01 00 00 08ncsi-geo tra
0070 1c 00 1d 00 6e 63 73 69 2d 67 65 6f 0e 74 72 61ncsi-geo tra
0080 66 66 69 63 6d 61 6e 61 67 65 72 03 6e 65 74 00 ...fficanana ger net...
0090 c0 35 00 05 00 01 00 00 eb b3 00 1d 03 77 77 77 755...www-m
00a0 00 6d 73 66 74 6e 63 73 69 03 63 6f 6d 09 65 64 ...msftncs i-com-ed
00b0 67 65 73 75 69 74 65 c0 4d c0 5e 00 05 00 01 00 ...gesuite- H...
00c0 00 00 55 00 12 85 63 31 39 36 31 02 67 32 06 61 ...-a1 961 g2-a
00d0 6b 61 6d 61 69 c0 4d c0 87 00 01 00 01 00 00 00 ...kanai-H...
00e0 0d 00 04 60 11 a8 6b c0 87 00 01 00 01 00 00 00 ...-k...
00f0 0d 00 04 60 11 a8 62b

2) Filter Used: dns.flags.response == 0

- **Observation:** Shows DNS queries.
- **Security Risk:** High query volume may indicate malware beaconing to C2 domains.
- **Recommendation:** Monitor unusual query spikes and block suspicious domains.

traffic_filters.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.flags.response == 0

No.	Time	Source	Destination	Protocol	Length	Info
5639	96.692520	192.168.1.3	192.168.1.1	DNS	87	Standard query 0x8a69 AAAA www.example.com
5645	96.695701	192.168.1.3	192.168.1.1	DNS	87	Standard query 0x51b3 HTTPS www.example.com
5647	96.695798	192.168.1.3	192.168.1.1	DNS	87	Standard query 0x99da A www.example.com
5662	96.770804	192.168.1.3	192.168.1.1	DNS	87	Standard query 0xabda A www.example.com
5664	96.770880	192.168.1.3	192.168.1.1	DNS	87	Standard query 0x7389 AAAA www.example.com
5668	96.771776	192.168.1.3	192.168.1.1	DNS	87	Standard query 0x50cd HTTPS www.example.com
5751	98.727697	2401:4900:1c73:7dc4...	2401:4900:50:9::201	DNS	95	Standard query 0xadd5 A www.example.com
5752	98.727797	2401:4900:1c73:7dc4...	2401:4900:50:9::201	DNS	95	Standard query 0x8515 AAAA www.example.com
5794	98.763060	2401:4900:1c73:7dc4...	2401:4900:50:9::205	DNS	95	Standard query 0x8515 AAAA www.example.com
5795	98.763060	2401:4900:1c73:7dc4...	2401:4900:50:9::205	DNS	95	Standard query 0xadd5 A www.example.com
5954	99.874060	2401:4900:1c73:7dc4...	2401:4900:50:9::205	DNS	128	Standard query 0x6616 AAAA functional.events.data.
5958	99.874797	2401:4900:1c73:7dc4...	2401:4900:50:9::205	DNS	128	Standard query 0xa66c HTTPS functional.events.data.
5962	99.875548	2401:4900:1c73:7dc4...	2401:4900:50:9::205	DNS	128	Standard query 0x5f4c A functional.events.data.mic
5989	100.899883	2401:4900:1c73:7dc4...	2401:4900:50:9::205	DNS	128	Standard query 0xf980 AAAA functional.events.data.
6006	101.567033	192.168.1.7	224.0.0.251	MDNS	279	Standard query 0x0000 ANY {"nm":"Redmi Note 9","as
6007	101.567526	fe80::d049:b6ff:fee...	ff02::fb	MDNS	299	Standard query 0x0000 ANY {"nm":"Redmi Note 9","as
6008	101.874510	192.168.1.7	224.0.0.251	MDNS	279	Standard query 0x0000 ANY {"nm":"Redmi Note 9","as
6009	101.875146	fe80::d049:b6ff:fee...	ff02::fb	MDNS	299	Standard query 0x0000 ANY {"nm":"Redmi Note 9","as
6013	102.079272	192.168.1.7	224.0.0.251	MDNS	279	Standard query 0x0000 ANY {"nm":"Redmi Note 9","as
6014	102.080029	fe80::d049:b6ff:fee...	ff02::fb	MDNS	299	Standard query 0x0000 ANY {"nm":"Redmi Note 9","as
6020	103.973262	2401:4900:1c73:7dc4...	2401:4900:50:9::201	DNS	94	Standard query 0x5f9a A ecs.office.com
6021	103.973659	2401:4900:1c73:7dc4...	2401:4900:50:9::201	DNS	94	Standard query 0x2c18 AAAA ecs.office.com
6087	110.066143	192.168.1.7	224.0.0.251	MDNS	279	Standard query 0x0000 ANY {"nm":"Redmi Note 9","as
6088	110.066675	fe80::d049:b6ff:fee...	ff02::fb	MDNS	299	Standard query 0x0000 ANY {"nm":"Redmi Note 9","as

> Frame 5962: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface 0

> Ethernet II, Src: 14:d4:24:19:d6:a9, Dst: 30:bd:13:36:25:50

> Internet Protocol Version 6, Src: 2401:4900:1c73:7dc4:7cdb:ae6:e5, Dst: 2401:4900:50:9::205

> Transmission Control Protocol, Src Port: 56149, Dst Port: 53, Seq: 1844674407370955360, Len: 128

> [2 Reassembled TCP Segments (56 bytes): #5961(2), #5962(54)]

> Domain Name System (query)

0000 30 bd 13 36 25 50 14 d4 24 19 d6 a9 86 dd 60 0c 00 06 P... s

0010 8c c3 00 4a 06 40 24 01 49 00 1c 73 7d c4 7c db ...J.@\$. I

0020 0a e6 e5 70 29 95 24 01 49 00 00 50 00 09 00 00 ...p).\$. I

0030 00 00 00 00 02 05 db 55 00 35 95 9d 31 06 62 98U .

0040 05 2a 50 18 ff ff 16 74 00 00 5f 4c 01 00 00 01 *P...t .

0050 00 00 00 00 00 00 0a 66 75 6e 63 74 69 6f 6e 61f u

0060 6c 06 65 76 65 6e 74 73 04 64 61 74 61 09 6d 69 l-events .

0070 63 72 6f 73 6f 66 74 03 63 6f 6d 00 00 01 00 01 crosoft . c

Frame (128 bytes) Reassembled TCP (56 bytes)

Response: Boolean

Packets: 15545 · Disposed: 668 (4.3%)

Profile: Default

3) Filter Used: dns.flags.response == 1

- **Observation:** Shows DNS responses.
- **Security Risk:** Malicious responses can redirect users to fake IPs (DNS spoofing).
- **Recommendation:** Use DNSSEC and trusted resolvers.

traffic_filters.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.flags.response==1

No.	Time	Source	Destination	Protocol	Length	Info
4869	84.057045	2401:4900:50:9::205	2401:4900:1c73:7dc4...	DNS	283	Standard query response 0xb1f1 AAAA www.bing.com C
4872	84.059058	2401:4900:50:9::205	2401:4900:1c73:7dc4...	DNS	259	Standard query response 0x23e0 A www.bing.com CNAM
5087	86.617264	192.168.1.7	224.0.0.251	MDNS	777	Standard query response 0x0000 PTR, cache flush Ar
5088	86.618456	fe80::d049:b6ff:fee...	ff02::fb	MDNS	797	Standard query response 0x0000 PTR, cache flush Ar
5279	89.045616	2401:4900:50:9::201	2401:4900:1c73:7dc4...	DNS	351	Standard query response 0x1bc3 AAAA storage.live.c
5391	90.136534	2401:4900:50:9::201	2401:4900:1c73:7dc4...	DNS	328	Standard query response 0x1bd6 AAAA login.live.com
5394	90.136534	2401:4900:50:9::201	2401:4900:1c73:7dc4...	DNS	393	Standard query response 0x68e8 A login.live.com CN
5548	94.604432	192.168.1.7	224.0.0.251	MDNS	777	Standard query response 0x0000 PTR, cache flush Ar
5549	94.605584	fe80::d049:b6ff:fee...	ff02::fb	MDNS	797	Standard query response 0x0000 PTR, cache flush Ar
5801	98.785344	2401:4900:50:9::205	2401:4900:1c73:7dc4...	DNS	205	Standard query response 0xadd5 A www.example.com C
5802	98.789767	2401:4900:50:9::205	2401:4900:1c73:7dc4...	DNS	229	Standard query response 0x8515 AAAA www.example.co
5939	99.214173	2401:4900:50:9::201	2401:4900:1c73:7dc4...	DNS	229	Standard query response 0x8515 AAAA www.example.co
5940	99.214173	2401:4900:50:9::201	2401:4900:1c73:7dc4...	DNS	205	Standard query response 0xadd5 A www.example.com C
5965	99.891787	2401:4900:50:9::205	2401:4900:1c73:7dc4...	DNS	301	Standard query response 0xa66c HTTPS functional.ev
5967	99.892028	2401:4900:50:9::205	2401:4900:1c73:7dc4...	DNS	257	Standard query response 0x5f4c A functional.events
5992	100.916703	2401:4900:50:9::205	2401:4900:1c73:7dc4...	DNS	312	Standard query response 0xf980 AAAA functional.eve
6016	102.386974	192.168.1.7	224.0.0.251	MDNS	777	Standard query response 0x0000 TXT, cache flush PT
6017	102.388040	fe80::d049:b6ff:fee...	ff02::fb	MDNS	797	Standard query response 0x0000 TXT, cache flush PT
6018	103.411212	192.168.1.7	224.0.0.251	MDNS	777	Standard query response 0x0000 TXT, cache flush PT
6019	103.412066	fe80::d049:b6ff:fee...	ff02::fb	MDNS	797	Standard query response 0x0000 TXT, cache flush PT
6022	103.979260	2401:4900:50:9::201	2401:4900:1c73:7dc4...	DNS	275	Standard query response 0x5f9a A ecs.office.com CN
6023	103.979260	2401:4900:50:9::201	2401:4900:1c73:7dc4...	DNS	299	Standard query response 0x2c18 AAAA ecs.office.com
6070	105.356710	192.168.1.7	224.0.0.251	MDNS	777	Standard query response 0x0000 TXT, cache flush PT
6071	105.357658	fe80::d049:b6ff:fee...	ff02::fb	MDNS	797	Standard query response 0x0000 TXT, cache flush PT

> Frame 5940: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interface 0

> Ethernet II, Src: 30:bd:13:36:25:50, Dst: 14:d4:24:19:d6:a9

> Internet Protocol Version 6, Src: 2401:4900:50:9::201, Dst: 2401:4900:1c73:7dc4::1

> User Datagram Protocol, Src Port: 53, Dst Port: 61218

> Domain Name System (response)

```

0000  14 d4 24 19 d6 a9 30 bd 13 36 25 50 00 00 00 00  ..$....0...
0010  00 00 00 97 11 3c 24 01 49 00 00 50 00 09 00 00  ....<$...I
0020  00 00 00 00 02 01 24 01 49 00 1c 73 7d c4 7c db  ....<$...I
0030  0a e5 e5 70 29 95 00 35 ef 22 00 97 b9 14 ad d5  ...p)...5...
0040  81 80 00 01 00 04 00 00 00 00 03 77 77 77 07 65  ....T...
0050  78 61 6d 70 6c 65 03 63 6f 6d 00 00 01 00 01 c0  xample.c o
0060  0c 00 05 00 01 00 00 01 2c 00 22 03 77 77 77 07  dgesuite
0070  65 78 61 6d 70 6c 65 06 63 6f 6d 2d 76 34 09 65  example.c o
0080  64 67 65 73 75 69 74 65 03 6e 65 74 00 c0 2d 00  dgesuite
0090  05 00 01 00 00 54 60 00 14 05 61 31 34 32 32 04  ....T...
00a0  64 73 63 72 06 61 6b 61 6d 61 69 c0 4a c0 5b 00  dscr-aka m
00b0  01 00 01 00 00 00 14 00 04 17 df f3 91 c0 5b 00  ....
00c0  01 00 01 00 00 00 14 00 04 17 df f3 71  ....

```

Ethernet (eth), 14 bytes

Packets: 15545 · Displayed: 320 (2.1%)

Profile: Default

4)Filter Used: dns.gry.name == "www.example.com"

- **Observation:** Filters queries for a specific domain.
- **Security Risk:** Could reveal targeted reconnaissance on particular domains.
- **Recommendation:** Monitor sensitive domains frequently queried inside the network.

traffic_filters.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.qry.name=="www.udemy.com"

No.	Time	Source	Destination	Protocol	Length	Info
9814	138.165210	2401:4900:1c73:7dc4...	2401:4900:50:9::201	DNS	105	Standard query 0xf252 A www.udemy.com
9820	138.167127	2401:4900:1c73:7dc4...	2401:4900:50:9::201	DNS	105	Standard query 0x3dc8 AAAA www.udemy.com
9822	138.167267	2401:4900:1c73:7dc4...	2401:4900:50:9::201	DNS	105	Standard query 0x5f0f HTTPS www.udemy.com
9825	138.171684	2401:4900:50:9::201	2401:4900:1c73:7dc4...	DNS	135	Standard query response 0x3dc8 AAAA www.udemy.com
9858	138.447037	2401:4900:1c73:7dc4...	2401:4900:50:9::201	DNS	105	Standard query 0x552d AAAA www.udemy.com
9864	138.447278	2401:4900:1c73:7dc4...	2401:4900:50:9::201	DNS	105	Standard query 0xd97c A www.udemy.com
9870	138.451997	2401:4900:50:9::201	2401:4900:1c73:7dc4...	DNS	135	Standard query response 0x552d AAAA www.udemy.com
10114	138.998037	2401:4900:1c73:7dc4...	2401:4900:50:9::201	DNS	105	Standard query 0x552d AAAA www.udemy.com
10116	138.998133	2401:4900:1c73:7dc4...	2401:4900:50:9::201	DNS	105	Standard query 0x4caf A www.udemy.com
10288	139.273695	2401:4900:1c73:7dc4...	2401:4900:50:9::201	DNS	105	Standard query 0x0e4d A www.udemy.com
10621	140.016117	192.168.1.3	192.168.1.1	DNS	85	Standard query 0x61c6 HTTPS www.udemy.com
10627	140.019029	2401:4900:1c73:7dc4...	2401:4900:50:9::201	DNS	105	Standard query 0x829c A www.udemy.com
10638	140.285341	192.168.1.3	192.168.1.1	DNS	85	Standard query 0x9c86 A www.udemy.com
11275	140.763763	192.168.1.3	192.168.1.1	DNS	85	Standard query 0xc1de AAAA www.udemy.com
11279	140.764905	192.168.1.3	192.168.1.1	DNS	85	Standard query 0x1fb4 A www.udemy.com
11290	140.772836	192.168.1.1	192.168.1.3	DNS	115	Standard query response 0xc1de AAAA www.udemy.com
11294	140.774523	192.168.1.1	192.168.1.3	DNS	119	Standard query response 0x1fb4 A www.udemy.com A 1
11500	141.025831	192.168.1.3	192.168.1.1	DNS	85	Standard query 0x41b5 A www.udemy.com
11506	141.027076	192.168.1.3	192.168.1.1	DNS	85	Standard query 0x3930 HTTPS www.udemy.com
11514	141.032343	192.168.1.1	192.168.1.3	DNS	119	Standard query response 0x41b5 A www.udemy.com A 1
14628	145.449299	2401:4900:1c73:7dc4...	2401:4900:50:9::205	DNS	105	Standard query 0x3925 A www.udemy.com
14631	145.449584	2401:4900:1c73:7dc4...	2401:4900:50:9::205	DNS	105	Standard query 0x83dd AAAA www.udemy.com
14647	145.466172	2401:4900:50:9::205	2401:4900:1c73:7dc4...	DNS	139	Standard query response 0x3925 A www.udemy.com A 1
15081	146.444750	192.168.1.3	192.168.1.1	DNS	85	Standard query 0x713d AAAA www.udemy.com

> Frame 9814: 105 bytes on wire (840 bits), 105 bytes captured (840) on interface eth0
 > Ethernet II, Src: 14:d4:24:19:d6:a9, Dst: 30:bd:13:36:25:50
 > Internet Protocol Version 6, Src: 2401:4900:1c73:7dc4:7cdb:ae6:e5, Dst: 2401:4900:50:9::201
 > Transmission Control Protocol, Src Port: 56303, Dst Port: 53, Seq: 1844674407370955360, Win: 65535, Len: 105
 > [2 Reassembled TCP Segments (33 bytes): #9813(2), #9814(31)]
 > Domain Name System (query)

```

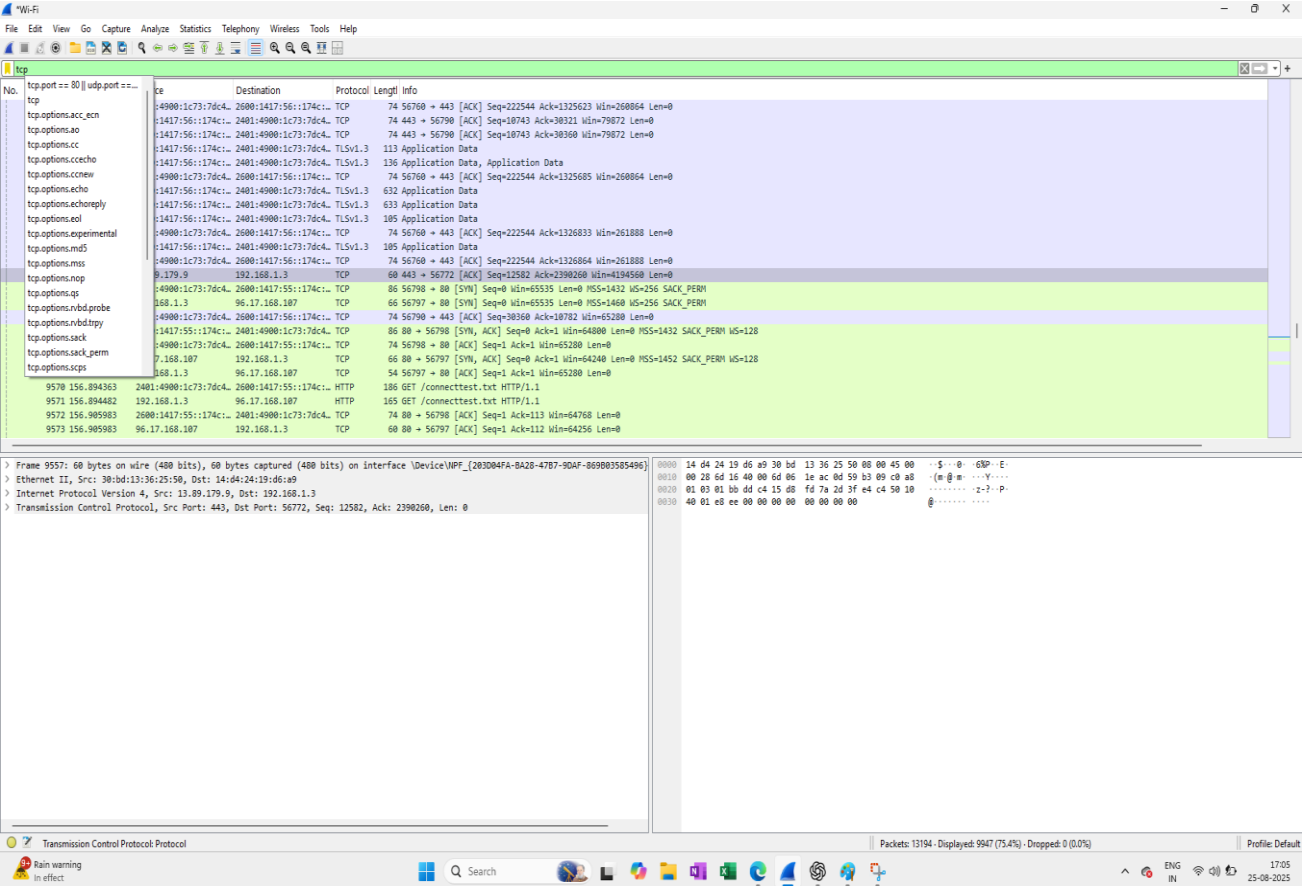
0000  30 bd 13 36 25 50 14 d4 24 19 d6 a9 86 dd 60 00  0...P...$
0010  92 c6 00 33 06 40 24 01 49 00 1c 73 7d c4 7c db  ...3...I
0020  0a e6 e5 70 29 95 24 01 49 00 00 50 00 09 00 00  ...p)...$
0030  00 00 00 00 02 01 db ef 00 35 aa 08 9c 64 65 11  ....
0040  0f 32 50 18 00 ff 50 17 00 00 f2 52 01 00 00 01  ..2P...P...
0050  00 00 00 00 00 00 03 77 77 77 05 75 64 65 6d 79  ....w...W
0060  03 63 6f 6d 00 00 01 00 01                    .com....
    
```

Frame (105 bytes) Reassembled TCP (33 bytes)

Ethernet (eth) 14 bytes Packets: 15545, Displayed: 25 (0.2%) Profile: Default

Filter Used: tcp

- **Observation:** Captures all TCP traffic.
- **Security Risk:** High traffic volume could hide scans, brute-force attempts, or data exfiltration.
- **Recommendation:** Baseline normal TCP traffic; alert on anomalies.



Filter Used: tcp.port == 80

- **Observation:** Captures traffic on port 80 (HTTP).
- **Security Risk:** Plaintext communication vulnerable to sniffing or man-in-the-middle attacks.
- **Recommendation:** Redirect all port 80 traffic to HTTPS (443).

The image shows a Wireshark packet capture window titled "traffic_filters.pcapng". The filter bar at the top displays "tcp.port==80". The packet list pane shows a series of captured packets, with the following details visible for packet 8330:

No.	Time	Source	Destination	Protocol	Length	Info
8330	134.033353	2401:4900:1c73:7dc4...	2600:140f:c400::173...	TCP	74	56147 → 80 [ACK] Seq=1 Ack=510 Win=65024 Len=0

The packet details pane for packet 8330 shows the following structure:

- > Ethernet II, Src: 14:d4:24:19:d6:a9, Dst: 30:bd:13:36:25:50
- > Internet Protocol Version 6, Src: 2401:4900:1c73:7dc4:7cdb:ae6:e5, Dst: 2600:140f:c400::173
- > Transmission Control Protocol, Src Port: 56147, Dst Port: 80, Seq: 1, Ack: 510, Win: 65024, Len: 0

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and TCP header.

Filter Used: tcp.analysis.retransmission

- **Observation:** Identifies TCP retransmissions (potential packet loss or congestion).
- **Security Risk:** May indicate DoS attacks, poor network quality, or misconfigured devices.
- **Recommendation:** Investigate high retransmission rates; optimize routing/firewall rules.

traffic_filters.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.analysis.retransmission

No.	Time	Source	Destination	Protocol	Length	Info
7834	128.566141	2401:4900:1c73:7dc4...	2a03:2880:f28a:1ca:...	TCP	74	[TCP Retransmission] 55037 → 443 [FIN, ACK] Seq=1
7835	128.566157	2401:4900:1c73:7dc4...	2a03:2880:f28a:ce:f...	TCP	74	[TCP Retransmission] 55045 → 443 [FIN, ACK] Seq=1
7836	128.566171	2401:4900:1c73:7dc4...	2a03:2880:f244:1c3:...	TCP	74	[TCP Retransmission] 55042 → 443 [FIN, ACK] Seq=1
7837	128.566186	2401:4900:1c73:7dc4...	2a03:2880:f244:c2:f...	TCP	74	[TCP Retransmission] 55036 → 443 [FIN, ACK] Seq=1
7838	128.566209	2401:4900:1c73:7dc4...	2a03:2880:f349:120:...	TCP	74	[TCP Retransmission] 55046 → 443 [FIN, ACK] Seq=1
7839	128.566226	2401:4900:1c73:7dc4...	2404:a800:6:55:face...	TCP	74	[TCP Retransmission] 55044 → 443 [FIN, ACK] Seq=1
8162	133.347800	2401:4900:1c73:7dc4...	2404:a800:6:213:fac...	TCP	74	[TCP Retransmission] 55038 → 443 [FIN, ACK] Seq=1
8163	133.347897	2401:4900:1c73:7dc4...	2404:a800:6:112:fac...	TCP	74	[TCP Retransmission] 55041 → 443 [FIN, ACK] Seq=1
8164	133.377970	2401:4900:1c73:7dc4...	2404:a800:6:262:fac...	TCP	74	[TCP Retransmission] 55043 → 443 [FIN, ACK] Seq=1
8165	133.378078	2401:4900:1c73:7dc4...	2a03:2880:f26e:1c1:...	TCP	74	[TCP Retransmission] 55040 → 443 [FIN, ACK] Seq=1
8166	133.378103	2401:4900:1c73:7dc4...	2a03:2880:f349:120:...	TCP	74	[TCP Retransmission] 55039 → 443 [FIN, ACK] Seq=1
8167	133.378123	2401:4900:1c73:7dc4...	2a03:2880:f28a:1ca:...	TCP	74	[TCP Retransmission] 55037 → 443 [FIN, ACK] Seq=1
8168	133.378142	2401:4900:1c73:7dc4...	2a03:2880:f28a:ce:f...	TCP	74	[TCP Retransmission] 55045 → 443 [FIN, ACK] Seq=1
8169	133.378162	2401:4900:1c73:7dc4...	2a03:2880:f244:1c3:...	TCP	74	[TCP Retransmission] 55042 → 443 [FIN, ACK] Seq=1
8170	133.378182	2401:4900:1c73:7dc4...	2a03:2880:f244:c2:f...	TCP	74	[TCP Retransmission] 55036 → 443 [FIN, ACK] Seq=1
8171	133.378199	2401:4900:1c73:7dc4...	2a03:2880:f349:120:...	TCP	74	[TCP Retransmission] 55046 → 443 [FIN, ACK] Seq=1
8172	133.378221	2401:4900:1c73:7dc4...	2404:a800:6:55:face...	TCP	74	[TCP Retransmission] 55044 → 443 [FIN, ACK] Seq=1
9831	138.197497	192.168.1.3	172.64.151.210	TCP	54	[TCP Retransmission] 55348 → 443 [FIN, ACK] Seq=2
13018	142.884021	192.168.1.3	13.127.247.216	TCP	66	[TCP Retransmission] 56400 → 443 [SYN] Seq=0 Win=6
13121	143.136149	192.168.1.3	13.127.247.216	TCP	66	[TCP Retransmission] 56414 → 443 [SYN] Seq=0 Win=6
13927	144.704371	2401:4900:1c73:7dc4...	2606:4700:8390:2425...	TCP	675	[TCP Retransmission] 56474 → 443 [PSH, ACK] Seq=19
14084	144.887122	192.168.1.3	13.127.247.216	TCP	66	[TCP Retransmission] 56400 → 443 [SYN] Seq=0 Win=6
14194	145.144212	192.168.1.3	13.127.247.216	TCP	66	[TCP Retransmission] 56414 → 443 [SYN] Seq=0 Win=6
14576	145.382143	2401:4900:1c73:7dc4...	2001:4860:4802:34:...	TCP	1506	[TCP Retransmission] 56510 → 443 [ACK] Seq=7405 Ad

> Frame 8172: 74 bytes on wire (592 bits), 74 bytes captured (592 b...
> Ethernet II, Src: 14:d4:24:19:d6:a9, Dst: 30:bd:13:36:25:50
> Internet Protocol Version 6, Src: 2401:4900:1c73:7dc4:7cdb:ae6:5...
> Transmission Control Protocol, Src Port: 55044, Dst Port: 443, Seq=...

0000 30 bd 13 36 25 50 14 d4 24 19 d6 a9 86 dd 60 03 00 6%P...
0010 79 1b 00 14 06 40 24 01 49 00 1c 73 d7 c4 7c db y...@\$. 1
0020 0a e6 e5 70 29 95 24 04 a8 00 00 06 00 55 fa ce ...p)\$.
0030 b0 0c 33 33 70 20 d7 04 01 bb 3a 66 9a 17 fa 3c ...33p ...
0040 ed cb 50 11 04 00 5d fe 00 00 ...P...]

This frame is a (suspected) retransmission: Label

Packets: 15545 · Disallowed: 132 (0.8%) Profile: Default

Filter Used: tcp.flags.syn == 1 && tcp.flags.ack == 0

- **Observation:** Captures initial SYN packets (connection attempts).
- **Security Risk:** A high volume of SYN packets may indicate SYN flood (DoS attack).
- **Recommendation:** Deploy SYN cookies and monitor for abnormal SYN patterns.

The image displays a Wireshark packet capture analysis of a SYN flood attack. The packet list shows a series of SYN packets from 192.168.1.3 to 192.168.1.1. The packet details for frame 8110 show the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers. The packet bytes pane shows the raw data of the frame.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
7977	130.128086	2401:4900:1c73:7dc4...	2401:4900:50:9::201	TCP	86	56259 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
7978	130.148889	2401:4900:1c73:7dc4...	2401:4900:50:9::201	TCP	86	56260 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
8053	130.883685	2401:4900:1c73:7dc4...	2401:4900:50:9::201	TCP	86	56261 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
8054	130.884107	2401:4900:1c73:7dc4...	2401:4900:50:9::201	TCP	86	56262 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
8075	131.717046	2401:4900:1c73:7dc4...	2401:4900:50:9::201	TCP	86	56263 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
8076	131.717514	2401:4900:1c73:7dc4...	2401:4900:50:9::201	TCP	86	56264 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
8087	131.795718	192.168.1.3	192.168.1.1	TCP	66	56265 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
8094	132.550056	2401:4900:1c73:7dc4...	2401:4900:50:9::201	TCP	86	56266 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
8100	132.740962	192.168.1.3	192.168.1.1	TCP	66	56267 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
8107	132.789385	192.168.1.3	192.168.1.1	TCP	66	56268 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
8108	132.789669	192.168.1.3	192.168.1.1	TCP	66	56269 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
8109	132.790050	192.168.1.3	192.168.1.1	TCP	66	56270 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
8110	132.790240	192.168.1.3	192.168.1.1	TCP	66	56271 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
8173	133.561461	192.168.1.3	192.168.1.1	TCP	66	56272 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
8180	133.752028	192.168.1.3	192.168.1.1	TCP	66	56273 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
8187	133.811038	2401:4900:1c73:7dc4...	2401:4900:50:9::205	TCP	86	56274 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
8188	133.811381	2401:4900:1c73:7dc4...	2401:4900:50:9::205	TCP	86	56275 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
8189	133.811632	2401:4900:1c73:7dc4...	2401:4900:50:9::205	TCP	86	56276 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
8243	133.837408	192.168.1.3	13.224.163.122	TCP	66	56277 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
8244	133.838888	2401:4900:1c73:7dc4...	2401:4900:50:9::205	TCP	86	56278 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
8245	133.839229	2401:4900:1c73:7dc4...	2401:4900:50:9::205	TCP	86	56279 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
8246	133.839441	2401:4900:1c73:7dc4...	2401:4900:50:9::205	TCP	86	56280 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
8293	133.875465	2401:4900:1c73:7dc4...	2a04:4e42:600::729	TCP	86	56281 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS
8340	134.578563	2401:4900:1c73:7dc4...	2401:4900:50:9::205	TCP	86	56282 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS

Packet Details (Frame 8110):

- > Frame 8110: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- > Ethernet II, Src: 14:d4:24:19:d6:a9, Dst: 30:bd:13:36:25:50
- > Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.1
- > Transmission Control Protocol, Src Port: 56271, Dst Port: 53, Seq=0, Win=65535, Len=0

Packet Bytes:

```

0000  30 bd 13 36 25 50 14 d4 24 19 d6 a9 08 00 45 00  0...6%P...
0010  00 34 6a 21 40 00 80 06 0d 4e c0 a8 01 03 c0 a8  4j!@...
0020  01 01 db cf 00 35 95 0b d5 4d 00 00 00 80 02  5...
0030  ff ff aa 5d 00 00 02 04 05 b4 01 03 03 08 01 01  5...
0040  04 02
  
```

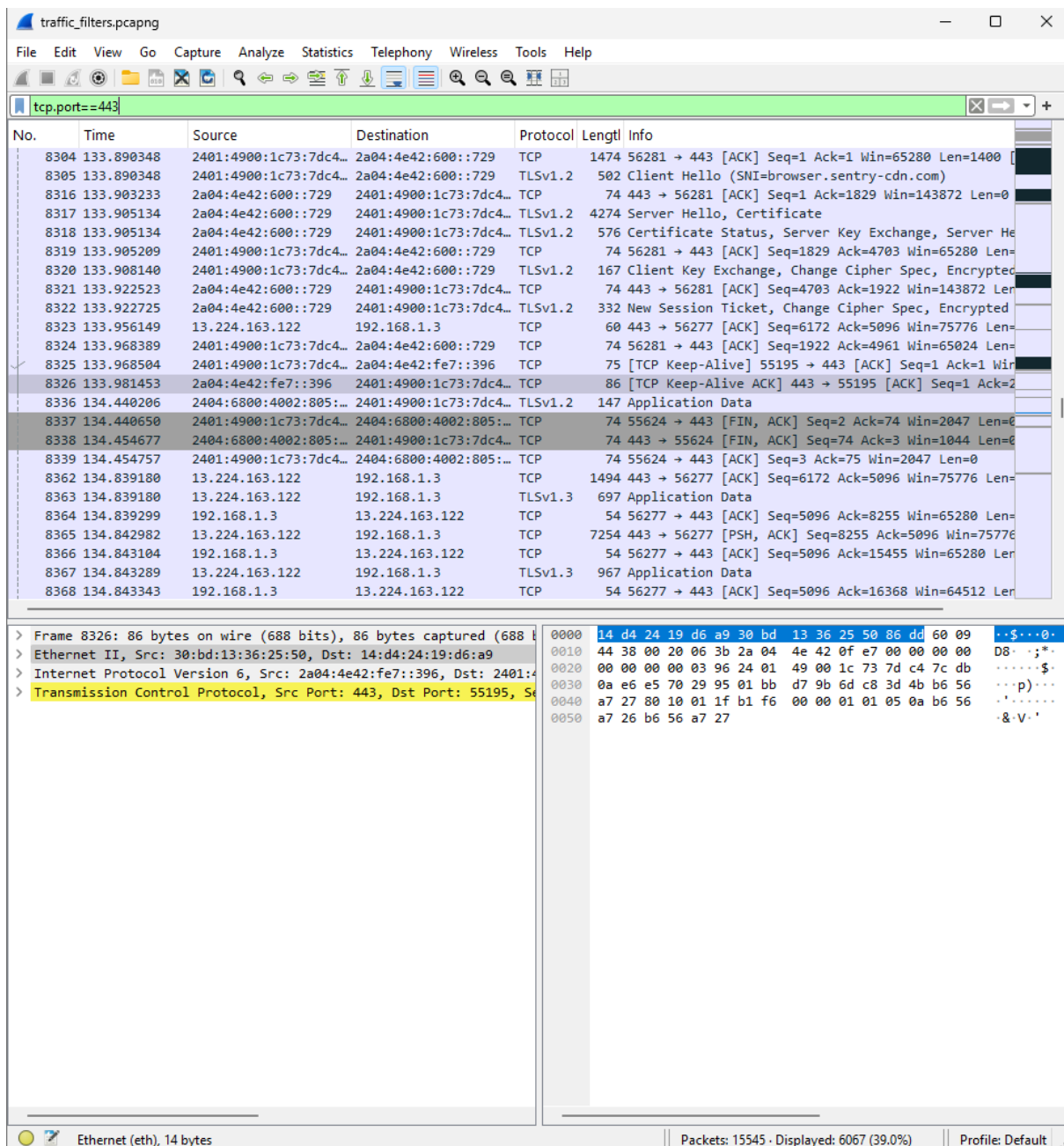
Bottom Status Bar:

- Ethernet (eth). 14 bytes
- Packets: 15545 · Displayed: 715 (4.6%)
- Profile: Default

TLS/HTTPS Filters

Filter Used: tcp.port == 443

- **Observation:** Captures HTTPS traffic.
- **Security Risk:** Content is encrypted, but metadata (IP, SNI, timing) can still leak info.
- **Recommendation:** Inspect TLS metadata; ensure modern cipher suites.



The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for common actions like opening files, saving, and filtering. The filter bar at the top shows the active filter: `tcp.port == 443`.

The packet list pane shows a series of captured packets. The selected packet is No. 8326, which is a TCP segment. The details pane for this packet shows the following structure:

- Frame 8326: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
- Ethernet II, Src: 30:bd:13:36:25:50, Dst: 14:d4:24:19:d6:a9
- Internet Protocol Version 6, Src: 2a04:4e42:fe7::396, Dst: 2401:4900:1c73:7dc4::729
- Transmission Control Protocol, Src Port: 443, Dst Port: 55195, Seq: 55195, Len: 86

The packet bytes pane shows the raw data of the selected packet, including the Ethernet II header, IP header, and TCP header. The TCP header shows the source port as 443 and the destination port as 55195.

Filter Used: ssl.handshake

- **Observation:** Captures TLS handshake messages (certificates, key exchange).
- **Security Risk:** Weak ciphers or expired certificates weaken encryption.
- **Recommendation:** Enforce TLS 1.2+ and disable weak ciphers.

The image shows a Wireshark packet capture window with the filter 'ssl.handshake' applied. The packet list on the left shows several TLS handshake messages (Client Hello, Server Hello, Change Cipher Spec, etc.) from various sources. The packet details pane on the right shows the structure of a TLS record, including the Client Hello message. The packet bytes pane at the bottom shows the raw data of the selected packet, including the TLS record structure and the Client Hello message.

No.	Time	Source	Destination	Protocol	Length	Info
6375	110.602667	192.168.1.3	204.79.197.219	TLSv1.3	340	Client Hello (SNI=r.msftstatic.com)
6389	110.613403	2600:140f:c400::173...	2401:4900:1c73:7dc4...	QUIC	1292	Initial, SCID=01b2ea983540fb22, PKN: 3, CRYPTO, PA
6404	110.619167	204.79.197.219	192.168.1.3	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
6405	110.620296	192.168.1.3	204.79.197.219	TLSv1.3	626	Change Cipher Spec, Client Hello (SNI=r.msftstatic
6409	110.625466	2401:4900:1c73:7dc4...	2600:140f:c400::173...	TLSv1.3	486	Client Hello (SNI=assets.msn.com)
6431	110.643635	204.79.197.219	192.168.1.3	TLSv1.3	1506	Server Hello
6439	110.647393	2600:140f:c400::173...	2401:4900:1c73:7dc4...	TLSv1.3	1506	Server Hello, Change Cipher Spec, Application Data
6842	111.812235	2401:4900:1c73:7dc4...	2600:1417:55::174c:...	QUIC	1292	Initial, DCID=57c6b0180e2507e8, PKN: 2, PADDING, C
6909	111.828827	2600:1417:55::174c:...	2401:4900:1c73:7dc4...	QUIC	1292	Initial, SCID=056234b9ad80281a, PKN: 3, CRYPTO, PA
7360	121.059965	2401:4900:1c73:7dc4...	2600:140f:2e00::b85...	TLSv1.3	817	Client Hello (SNI=r.bing.com)
7376	121.074698	2600:140f:2e00::b85...	2401:4900:1c73:7dc4...	TLSv1.3	338	Server Hello, Change Cipher Spec, Application Data
7930	129.877722	192.168.1.3	18.164.188.113	TLSv1.3	385	Client Hello (SNI=d3njcbbhojbot.cloudfront.net)
7959	129.890930	18.164.188.113	192.168.1.3	TLSv1.3	5814	Server Hello, Change Cipher Spec, Application Data
8257	133.851920	192.168.1.3	13.224.163.122	TLSv1.3	372	Client Hello (SNI=www.coursera.org)
8271	133.865454	13.224.163.122	192.168.1.3	TLSv1.3	4374	Server Hello, Change Cipher Spec, Application Data
8305	133.890348	2401:4900:1c73:7dc4...	2a04:4e42:600::729	TLSv1.2	502	Client Hello (SNI=browser.sentry-cdn.com)
8317	133.905134	2a04:4e42:600::729	2401:4900:1c73:7dc4...	TLSv1.2	4274	Server Hello, Certificate
8318	133.905134	2a04:4e42:600::729	2401:4900:1c73:7dc4...	TLSv1.2	576	Certificate Status, Server Key Exchange, Server He
8320	133.908140	2401:4900:1c73:7dc4...	2a04:4e42:600::729	TLSv1.2	167	Client Key Exchange, Change Cipher Spec, Encrypted
8322	133.922725	2a04:4e42:600::729	2401:4900:1c73:7dc4...	TLSv1.2	332	New Session Ticket, Change Cipher Spec, Encrypted
8375	134.935581	192.168.1.3	18.164.188.113	TLSv1.3	353	Client Hello (SNI=d3njcbbhojbot.cloudfront.net)
8377	134.953423	18.164.188.113	192.168.1.3	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
8865	136.254599	2401:4900:1c73:7dc4...	2404:6800:4002:81a:...	QUIC	1292	Initial, DCID=3fbc538a01a0609, PKN: 2, PADDING, F
8877	136.272406	2404:6800:4002:81a:...	2401:4900:1c73:7dc4...	QUIC	1292	Initial, SCID=ffbc538a01a0609, PKN: 3, CRYPTO, PA

Frame 7959: 5814 bytes on wire (46512 bits), 5814 bytes captured
Ethernet II, Src: 30:bd:13:36:25:50, Dst: 14:d4:24:19:d6:a9
Internet Protocol Version 4, Src: 18.164.188.113, Dst: 192.168.1.3
Transmission Control Protocol, Src Port: 443, Dst Port: 56255, Seq: 3441111111, Len: 5814
Transport Layer Security

0000 14 d4 24 19 d6 a9 30 bd 13 36 25 50 08 00 45 00 ..\$....0
0010 16 a8 c8 78 00 00 fa 06 51 16 12 a4 bc 71 c0 a8 ...x...
0020 01 03 01 bb db bf b2 34 bc f0 29 f8 45 06 50 18 ...b...
0030 00 87 00 55 00 00 16 03 03 04 ba 02 00 04 b6 03 ...U...
0040 03 8b ae 1f 11 af 44 c9 d8 95 f1 ea 9e 75 12 8c ...D...
0050 fc 4d d2 36 f5 43 85 cc 0b f5 c6 5f f4 c2 59 14 ...M-6-C...
0060 f0 20 80 67 b4 90 73 1a f3 f9 03 11 3e 37 d7 36 ...g...s...
0070 f1 3e 48 64 33 10 af 60 df cb 17 01 0a b3 ab 2a ...>Hd3...
0080 9e 22 13 01 00 04 6e 00 2b 00 02 03 04 00 33 04 ..."....n...
0090 64 11 ec 04 60 11 da 97 98 1d 32 da 82 f4 e0 b6 ...d...
00a0 c4 c8 36 7d d8 71 24 8a 54 4c 95 72 2a 49 e0 dd ...6}..q\$...
00b0 27 12 a9 72 a2 c7 03 32 43 03 cc 58 de 29 a3 61 ...b...
00c0 d0 31 8f 69 23 2d 32 00 f6 1f 82 16 3d 5b a8 f5 ...1-i#-2...
00d0 21 7d d4 90 3c a3 5c 74 fc ae 40 3f c9 af 34 e2 ...!}<<<\t...
00e0 a6 8a a7 6b 3c 94 cd c8 2a d0 2c c8 bb d1 ba 9f ...<k...
00f0 97 e2 31 33 93 f4 19 48 36 56 49 6a ff 43 0b c1 ...13...t...
0100 01 5e b5 e3 31 05 12 b8 d6 fe 05 78 2f 6f 36 e4 ...^..1...
0110 22 6a 1f c9 43 98 23 c5 2b e6 4c 65 13 68 1b 27 ...f}..C.#...
0120 b8 62 85 3d 03 91 a1 3d 13 b2 19 4a dc 3c c0 7e ...b...
0130 c1 9e 1e d9 b5 80 72 6e f2 53 bd 34 12 e0 4c 5e ...<...r...
0140 a6 21 d1 05 3c cf c0 8d 86 22 34 a9 fc d3 48 56 ...!<...<...
0150 02 16 6a ff 7a 81 24 69 0d d6 86 27 32 c2 89 e8 ...j..z:\$...
0160 be 5a 5e aa eb 08 2f 8c 8d ee 6c b3 ad 27 0d 73 ...Z^.../...
0170 81 0b aa 12 83 06 16 0c 2d fa 62 d5 9c 45 ac 1a ...D...f...
0180 61 1e a9 52 c9 98 1d 09 a4 c8 ef e0 54 e5 ca 5a ...a..R...
0190 59 d0 32 69 10 25 e5 6a 10 78 c0 b0 89 01 82 e1 ...Y-21-%...
01a0 b6 84 44 e0 c4 b0 b6 46 03 f8 eb 3e a4 db 92 1e ...D...f...
01b0 21 f0 4b 50 55 dc 9e 9d e2 81 d3 bf c9 98 92 a5 ...!..KPU...
01c0 8d b8 be 23 ef 9a f6 9b 92 4b 8a a5 56 b0 0e ee ...#...</p></div>